

**UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF ILLINOIS**

VICTORIA EDELSTEIN, Individually and )  
On Behalf of All Others Similarly Situated, )

Case No.

Plaintiff,

## CLASS ACTION COMPLAINT

VS.

## DEMAND FOR JURY TRIAL

FACEBOOK, INC.,

Defendant.

**CLASS ACTION COMPLAINT FOR VIOLATIONS OF THE ILLINOIS BIOMETRIC  
INFORMATION PRIVACY ACT**

Plaintiff Victoria Edelstein, individually and on behalf of all others similarly situated, through undersigned counsel, brings this Class Action Complaint for Violations of the Illinois Biometric Information Privacy Act (“BIPA”), 740 ILCS 14/1 *et seq.*, against defendant Facebook, Inc. (“Facebook” or “Defendant”), and alleges the following upon information and belief, except as to the allegations within Plaintiff’s personal knowledge. Plaintiff believes that substantial additional evidentiary support will exist for the allegations set forth herein after a reasonable opportunity for discovery.

## SUMMARY OF THE ACTION

1. Facebook, Inc. is a social media conglomerate founded in 2004. It owns its eponymous social networking platform in addition to a host of subsidiaries.

2. Instagram is a photo and video-sharing social networking service that is owned by Facebook, Inc. It was initially released as an application for the iOS mobile operating system in 2010 before being acquired by Facebook in 2012. Since its acquisition by Facebook, Instagram has steadily amassed new users worldwide. In 2019, there were more approximately

118 million users in the United States alone.

3. Facebook's social media platform offers a multi-faceted approach for users to connect with one another. In addition to sharing photos and videos, Facebook is a social networking service which allows users to share news articles, create special interest groups, shop, and more. Instagram, on the other hand, is more limited in its scope of use. Its primary features are photo and video sharing, direct messaging, and "stories," which are photos and/or videos which disappear from a user's profile after 24 hours.

4. Earlier this year Facebook agreed to pay \$650 million to settle a class action that accuses the company of illegally harvesting the protected biometrics of users of its Facebook platform. As set forth below, Facebook also illegally harvests the protected biometrics of users of its Instagram application.

5. In direct violation of Sections 15(a)-(e) of the BIPA, Facebook is actively collecting, storing, disclosing, profiting from, and otherwise using the biometric information of its reportedly more than 100 million Instagram users without any written notice or informed written consent, including millions of Illinois residents.

6. Facebook has readily admitted to its collection of biometrics from Instagram users. Its facial recognition software works by scanning faces of unnamed people in photos or videos to analyze details of individuals' faces and creating a corresponding "face template" for each face, and then storing that face template for later use and/or matching it to those already in a database of identified people. Facebook has said that users are in charge of that process, but in reality, people cannot actually control the technology because Facebook scans their faces in photos and videos uploaded by other users, even if their individual facial recognition setting is

turned off.<sup>1</sup>

7. Facebook surreptitiously captures its Instagram users' protected biometrics without their informed consent and, worse yet, without actually informing them of its practice. Upon information and belief, once Facebook captures its Instagram users' protected biometrics, it uses them to bolster its facial recognition abilities across all of its products, including the Facebook application, and shares this information among various entities. Facebook does all of this without providing any of the required notices or disclosures required by Illinois law.

8. Plaintiff brings this action individually and on behalf of a proposed class in order to stop Facebook's violations of the BIPA and to recover statutory damages for Facebook's unauthorized collection, storage, disclosure, profiting from, and use of their biometric information in violation of the BIPA.

#### **PARTIES**

9. Plaintiff Victoria Edelstein is, and has been at all relevant times, a resident and citizen of the state of Illinois and a resident of Lake County, Illinois. Plaintiff first created an Instagram account in 2017 and has used Instagram regularly since that time.

10. During the relevant time period, Ms. Edelstein accessed Instagram on both her computer and phone to post photographs, view content posted by other users, and react to that content via comments and "likes." Ms. Edelstein frequently tagged herself and others in photographs posted on Instagram and appeared in photographs uploaded by others to Instagram. Plaintiff was not aware that any facial recognition data or other biometric data was being collected by Facebook through her Instagram use.

11. Defendant Facebook is a Delaware corporation with its headquarters and principal executive offices at 1601 Willow Road, Menlo Park, California 94025. Facebook is a

---

<sup>1</sup> See <https://www.nytimes.com/2018/07/09/technology/facebook-facial-recognition-privacy.html>

citizen of the states of Delaware and California. Facebook is also registered to conduct business in the State of Illinois (file number 66267067) and maintains an office in Cook County.

### **JURISDICTION AND VENUE**

12. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. §1332 in that Plaintiff and Defendant are citizens of different states and the amount in controversy exceeds \$75,000, exclusive of interests and costs.

13. Jurisdiction is also proper in this Court pursuant to the Class Action Fairness Act, 28 U.S.C. §1332(d) (“CAFA”), because: (i) the proposed class consists of well over 100 members; (ii) the parties are minimally diverse, as members of the proposed class, including plaintiff, are citizens of a state different from Defendant’s home states; and (iii) the aggregate amount in controversy exceeds \$5,000,000, exclusive of interests and costs. There are millions of estimated Instagram users in the state of Illinois. The estimated number of Illinois Instagram users impacted by Defendant’s conduct multiplied by BIPA’s statutory liquidated damages figure (\$5,000 for each intentional or reckless violation and \$1,000 for each negligent violation) easily exceeds CAFA’s \$5,000,000 threshold.

14. Venue is proper in this District because Defendant is registered to conduct business in Illinois, conducts business transactions in this District, and the causes of action arose, in substantial part, in this District. Venue is additionally proper because plaintiff resides in this District.

### **SUBSTANTIVE ALLEGATIONS**

#### **I. Biometric Information and the Illinois BIPA**

15. A “biometric identifier” is any personal feature that is unique to an individual

including fingerprints, iris scans, DNA, facial features and voice, among others.<sup>2</sup>

16. The Illinois Legislature has found that “[b]iometrics are unlike other unique identifiers that are used to access finances or other sensitive information.” 740 ILCS 14/5(c). “For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions.” *Id.*

17. In recognition of this legitimate concern over the security of biometric information, the Illinois Legislature enacted the BIPA, which provides, *inter alia*, that:

No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person’s or a customer’s biometric identifier or biometric information, ***unless it first:***

(1) ***informs*** the subject or the subject’s legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored;

(2) ***informs*** the subject or the subject’s legally authorized representative in writing of the ***specific purpose and length of term*** for which a biometric identifier or biometric information is being collected, stored, and used; ***and***

(3) receives a ***written release*** executed by the subject of the biometric identifier or biometric information or the subject’s legally authorized ***representative***.

740 ILCS 14/15(b).

18. Section 15(a) of the BIPA further provides that:

A private entity in possession of biometric identifiers or biometric information ***must develop a written policy, made available to the public***, establishing a retention schedule and guidelines for permanently destroying biometric

---

<sup>2</sup> The BIPA defines “biometric information” as “any information, regardless of how it is captured, converted, stored, or shared, based on an individual’s biometric identifier used to identify an individual. Biometric information does not include information derived from items or procedures excluded under the definition of biometric identifiers.” 740 ILCS 14/10. Plaintiff herein uses the terms “biometric information” and “biometric identifier” interchangeably.

identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first.

740 ILCS 14/15(a).

19. As alleged herein, Facebook's practices of collecting, storing, and using Instagram users' biometric information without informed written consent violates all three prongs of §15(b) of the BIPA. Facebook's failure to provide a publicly available written policy regarding its schedule and guidelines for the retention and permanent destruction of Instagram users' biometric information within the earlier of 3 years of a user's last interaction with Facebook or whenever the initial purpose for collecting the biometric information is satisfied violates §15(a) of the BIPA.

20. Facebook has also violated Section 15(c) of the BIPA by selling, leasing, trading, or otherwise profiting from a person's biometrics, as set forth more fully below.

21. Facebook has likewise violated Sections 15(d)-(e) of the BIPA by disclosing, redisclosing, or otherwise disseminating the biometrics captured from media uploaded to Instagram, as set forth more fully below.

## **II. Facebook Collects, Stores, Discloses, Profits from, and Otherwise Uses Plaintiffs' and Class Members' Biometric Information in Violation of the BIPA**

22. Instagram has over one billion users worldwide and millions of users in Illinois alone.

23. Instagram allows its users to create a personal page where members can upload photographs and videos, participate in live video broadcasts, and communicate and interact with other Instagram users. Approximately 95 million photos are shared on Instagram each day, with over 40 billion photos and videos shared on the platform since its inception.

24. Facebook has employed its facial recognition technology continuously from the time it was first introduced in 2010, including the time period after its acquisition of Instagram in 2012, and continuing to the date of the filing of this Complaint.

25. Facebook's sophisticated facial recognition technology works by collecting and analyzing the facial features of individuals appearing in photographs and videos uploaded to Instagram and generating a "biometric signature" or "face template" of each individual's face that appears therein. This facial template is based on each person's facial geometry and is specific to that person. Facebook, upon information and belief, stores those face templates taken from Instagram in a large database of face templates, which database additionally includes face templates Facebook has made from photographs its users have uploaded to other platforms besides Instagram, including photographs uploaded to Facebook. As Facebook's Instagram and Facebook users continue to manually tag friends, family, and other people they recognize in a photograph, Facebook's software automatically compares those images to the face templates in its database. If there is a match, Facebook may identify the user.

26. Facebook is then able to identify the individuals whose biometrics it has captured by cross referencing the face templates of individuals appearing in Instagram photographs with face templates that it has already linked with an identified individual (for instance, face templates taken from a face that Instagram or Facebook users have tagged, or with face templates that have been identified via other platforms or companies that Facebook shares its protected biometrics with), and identify the individual when there is a match.

27. Prior to January 1, 2020, Facebook has never informed Instagram users that it collects their biometric data. Rather, the Instagram Data Policy merely states that Facebook collects information "you and others provide" to the app, in the form of both posted content and

anything users might see through the camera, and that its systems *automatically process* the content and communications provided by users *to analyze context and what's in them* (emphasis added).<sup>3</sup>

28. In fact, Facebook actively mislead Instagram users about whether it was collecting facial recognition data. Instagram's Data Policy states, "If you have it turned on, we use face recognition technology to recognize you in photos, videos and camera experiences."<sup>4</sup> However, Instagram users have no ability to turn off any facial recognition software within the app. Furthermore, the Instagram Data Policy states, "If we introduce face-recognition technology to your Instagram experience, we will let you know first, and you will have control over whether we use this technology for you."<sup>5</sup> As set forth below, these statements are untrue.

29. On January 1, 2020, Facebook published, for the first time, its California Privacy Notice for its California users as a supplement to its current Data Policy in compliance with California's Consumer Privacy Act (CCPA).<sup>6</sup> Instagram admits in this notice that any of the information disclosed within the California Privacy Notice may have been collected from users over the past 12 months. While only California currently requires these types of disclosures to consumers, the contents of the notice demonstrate that Facebook has been collecting biometric data from its Instagram users for, at minimum, the 2019 calendar year. The California Privacy Notice is reproduced in part below (emphasis added):

<b>Categories of Personal Information we collect may include:</b>	<b>Examples of how Personal Information is used include:</b>	<b>Parties with whom your information may be shared include:</b>
---	--	--

<sup>3</sup> See <https://help.instagram.com/155833707900388> Section I: What Kinds of Information Do We Collect?

<sup>4</sup> See <https://help.instagram.com/519522125107875> Section II: How Do We Use This Information?

<sup>5</sup> *Id.*

<sup>6</sup> See <https://help.instagram.com/2482657248648591> "California Privacy Notice"



<ul style="list-style-type: none"> <li>• <b>Identifiers;</b></li> <li>• Data with special protections, if you choose to provide it;</li> <li>• Commercial information, if you choose to provide it;</li> <li>• <b><i>Photos and face imagery that can be used to create face-recognition templates if you or others choose to provide it and you have the setting turned on.</i></b></li> <li>• Internet or other electronic network activity information, including content you view or engage with;</li> <li>• Location-related information, including precise device location if you choose to allow us to collect it;</li> <li>• <b><i>Audio or visual Information, including photos and videos, if you or others choose to provide it;</i></b></li> <li>• Professional or employment information, if you choose to provide it;</li> <li>• Education information, if you choose to provide it;</li> <li>• Financial information, if you choose to provide it; and</li> </ul>	<ul style="list-style-type: none"> <li>• Providing, personalizing, and improving our Products;</li> <li>• Facilitating transactions, providing measurement, analytics, advertising, and other business services;</li> <li>• Promoting safety, integrity, and security;</li> <li>• Communicating with you;</li> <li>• Researching and innovating for social good; and</li> <li>• To perform other business purposes.</li> </ul>	<ul style="list-style-type: none"> <li>• People and accounts you share and communicate with;</li> <li>• People and accounts with which others share or reshare content about you;</li> <li>• Apps, websites, and third-party integrations on or using our Products;</li> <li>• New owners in the event of a change of ownership or control of all or part of our Products or their assets changes;</li> <li>• Partners, including partners who use our analytics services, advertisers, measurement partners, partners offering goods and services in our Products, vendors and service providers, and researchers and academics;</li> <li>• Law enforcement or other third parties in connection with legal requests; and</li> <li>• Facebook Companies.</li> </ul>
--	--	--

<ul style="list-style-type: none"> <li>Information derived from other Personal Information about you, which could include your preferences, interests, and other information used to personalize your experience.</li> </ul>		
--	--	--

30. Although Facebook’s California Privacy Notice indicates that it collects Instagram user’s protected biometrics “if you or others choose to provide it and you have the setting turned on,” Facebook’s belated after-the-fact notice to Instagram users cannot constitute compliance with the BIPA for a variety of reasons, including that Facebook only allowed Class Members’ to opt out *after* it collected their protected biometrics, and even then, only if Class Members knew to look for the opt-out option, which, upon information and belief, is not even possible through a user’s *Instagram* account.<sup>7</sup>

31. In any event, Instagram users *cannot* opt out. Indeed, Instagram users are not even given an opportunity to provide a written release because Facebook automatically processes content and shares it across its platforms. Rochelle Nadhiri, a Facebook spokeswoman, said its system analyzes faces in users’ photos to check whether they match with those who have their facial recognition setting turned on. This means that users can never really “opt out” of Facebook’s use of facial recognition. Even if a user does not have facial recognition activated on their personal account, their photo may still be scanned, collected, and entered into Facebook’s database if it matches with a user’s data who does have the facial

<sup>7</sup> See <https://help.instagram.com/519522125107875>, directing Instagram users to “opt out” via settings on their Facebook profile.

recognition setting activated.<sup>8</sup> This further means that one can never truly “opt out” because Facebook must capture and compare the biometrics of a face before learning if that face in fact matches with faces of users who have their facial recognition setting turned on or off.

32. Further, Facebook concedes that it collects information such as the location of a photo, Instagram users’ current location, where they live, the places they go, and the businesses and people they’re near-to to “provide, personalize and improve our Products.” As such Facebook knows, or should know, that Plaintiffs’ and Class Members are Illinois users.<sup>9</sup>

33. Moreover, upon information and belief, Facebook disclosed Instagram users’ protected facial templates not only across various teams operating across its own various platforms, but with third parties. Facebook concedes that biometrics harvested from Instagram’s photographs and videos may be shared with other apps, websites, and third-party integrations, Facebook’s partners, including partners who use Facebook’s analytics services, advertisers, measurement partners, partners offering goods and services in Facebook’s products, vendors and service providers, researchers and academics, law enforcement, and Facebook Companies, including Facebook Payments Inc., Onavo, Facebook Technologies, LLC and Facebook Technologies Ireland Limited, WhatsApp Inc., WhatsApp Ireland Limited, and CrowdTangle.<sup>10</sup>

34. Facebook and Instagram share infrastructure, systems, and technology with other Facebook Companies and process information about the user across the Facebook Companies.<sup>11</sup> This includes, upon information and belief, using Facebook’s facial recognition technology to process biometrics collected from Instagram users, which is then used to create new facial

---

<sup>8</sup> See <https://www.nytimes.com/2018/07/09/technology/facebook-facial-recognition-privacy.html>

<sup>9</sup> See <https://help.instagram.com/155833707900388>

<sup>10</sup> See <https://help.instagram.com/2482657248648591>

<sup>11</sup> See <https://help.instagram.com/155833707900388> Section IV: How Do the Facebook Companies Work Together?

templates and/or enhance already-existing facial templates of those users.

35. For example, Facebook is currently the subject of antitrust litigation in Germany, where they are alleged to have broken competition laws by combining personal data collected about users across its different platforms, including Instagram, to create “super profiles” for users.<sup>12</sup> A ruling from German regulators prohibited Facebook from combining Facebook user account data with user data on company services like WhatsApp and Instagram.<sup>13</sup>

36. Upon information and belief, Facebook’s shared infrastructure, systems, and technology and processing of user information across the Facebook Companies includes using the face templates harvested from its Instagram’s users’ uploaded material to improve the algorithms that power its facial recognition abilities across all of its platforms, including but not limited to its Facebook application where, for example, Facebook uses its facial recognition to suggest tags to Facebook users and lets Facebook users know when their photographs are uploaded by someone else.<sup>14</sup>

37. Upon information and belief, Facebook also includes the face templates captured from Instagram users’ uploaded material, as well as Instagram users’ tagging information, to bolster its databases of face templates and tagging information that enables Facebook’s facial recognition to continue learning and improving, which in turn enhances all of Facebook’s facial recognition products, including, for example, its predictive tagging feature on the Facebook application.<sup>15</sup> Several of Facebook’s products, such as Moments, an application Facebook

---

<sup>12</sup> See <https://www.nytimes.com/2020/06/23/technology/facebook-antitrust-germany.html>

<sup>13</sup> See <https://www.nytimes.com/2019/02/07/technology/germany-facebook-data.html>

<sup>14</sup> See <https://www.facebook.com/help/122175507864081> What is the face recognition setting on Facebook and how does it work?

<sup>15</sup> See <https://www.npr.org/sections/alltechconsidered/2016/05/18/477819617/facebooks-facial-recognition-software-is-different-from-the-fbis-heres-why#:~:text=Facebook-.Facebook's%20Moments%20app%20uses%20facial%20recognition%20technology%20to%20group%20photos,friend%20who%20are%20in%20them.&text=When%20someone%20tags%20you%20in,reminder%20of%20a%20sha>

introduced in 2015, capitalizes on Facebook's facial recognition technology.<sup>16</sup>

38. Several of Facebook's prior patent filings further attest to Facebook's commercial purposes in developing its facial recognition technologies. These patents reportedly described one system that could detect consumers within stores and match those shoppers' faces with their social networking profiles and another in which cameras near checkout counters could capture shoppers' faces and match them with their social networking profiles.<sup>17</sup>

39. As such, Facebook profits from its use of its Instagram users' protected biometrics by using them to improve the accuracy of its own facial recognition services, to expand the datasets which enable its facial recognition software, and to cement its market-leading position in facial recognition and social media.

40. In direct contravention of §15(a) of the BIPA, Facebook has collected Plaintiff's and Class Members' face templates without developing a written policy establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting such identifiers or information has been satisfied or within 3 years of the individual's last interaction with Facebook.

41. In direct contravention of §15(b) of the BIPA, Facebook collected Plaintiff's and Class Members' face templates without informing them that it would collect, store, and use their biometric facial information, without informing Instagram users of the specific purpose and length of term for which their biometric information would be collected, stored, and used, and without receiving a written release from Instagram users before it began to collect, store,

---

[redacted memory](#). (describing the benefit to facial recognition algorithms of additional photographs and tagging information).

<sup>16</sup> See <https://techcrunch.com/2015/06/15/facial-recogbook/>

<sup>17</sup> See <https://www.nytimes.com/2018/07/09/technology/facebook-facial-recognition-privacy.html>

disclose, profit from, and otherwise use their biometric information.

42. In direct contravention of §15(c) of the BIPA, Facebook profited from Plaintiff's and Class Members' protected face templates.

43. In direct contravention of §15(d)-(e) of the BIPA, Facebook voluntarily disclosed and otherwise disseminated Plaintiff's and Class Members' protected face templates.

### **Plaintiff's and Class Members' Injuries and Damages**

44. As alleged herein, as a result of Facebook's unlawful conduct, Plaintiff and Class Members have already sustained injuries and face many more imminent and certainly impending injuries, which injuries they will continue to suffer.

45. Facebook's unlawful conduct has resulted in, among other things: (a) Plaintiff's and Class Members' unique biometric identifiers and information being collected, captured, obtained, disclosed, and otherwise disseminated without the requisite notice having been given and without the requisite releases having been obtained; and (b) Plaintiff and Class Members being deprived of the very control over their biometric identifiers and information that BIPA was designed to protect.

46. To this day, Plaintiff and Class Members do not know which, or how many, individuals or entities have received, obtained, accessed, stored, disclosed, or otherwise made use of Plaintiff's and Class Members' biometric identifiers and information, exposing them to the imminent and certainly impending injuries of identity theft, fraud, stalking, surveillance, social engineering, and other invasions of privacy.<sup>18</sup>

47. As a result of Facebook's misconduct, Plaintiff and Class Members have no recourse for the fact that their biologically unique information has been compromised.

---

<sup>18</sup> *Facial Recognition Tech: 10 Views on Risks and Rewards*, <https://www.forbes.com/sites/forbestechcouncil/2018/04/03/facial-recognition-tech-10-views-on-risks-and-rewards/#54d3e1716b3c>

Moreover, Plaintiff and Class Members are likely to withdraw from biometric-facilitated transactions and other facially-mediated electronic participation.

### **III. Plaintiff's Personal Experiences**

48. Plaintiff is a resident of Mundelein, Illinois. In December of 2017, Plaintiff signed up for an Instagram account in Mundelein, Illinois in 2017, and has since then uploaded numerous photographs.

49. Since joining Instagram, Plaintiff has uploaded and posted many photographs to Facebook's network from Instagram that include images of her face, and Plaintiff has tagged herself in many of those photographs. Plaintiff's face has also appeared in many photographs that other Instagram users have uploaded to Instagram, and Plaintiff's face has been tagged by other Instagram users in many such photographs.

50. Many of these photographs were taken in Illinois and were uploaded from Plaintiff's computer in Illinois.

51. As is the case for Class Members, Facebook has, upon information and belief, captured biometric identifiers and information from Plaintiff's photographs by automatically locating and scanning Plaintiff's face, and by extracting geometric data relating to the contours of her face and the distances between her eyes, nose, and ears, data which Facebook then used to create a unique template of Plaintiff's face, as set forth more fully below.

52. The resulting unique face template was, upon information and belief, stored and used by Facebook for research purposes to develop its own facial recognition technologies across the various services and products it offers in connection with its Facebook Companies.

53. Facebook stores, discloses, profits from, and otherwise uses these face templates without Plaintiff's knowledge or consent.

54. Plaintiff did not receive notice that Facebook would collect, store, profit from, disclose, or otherwise use her biometric information when she used the Instagram app.

55. Plaintiff never provided informed consent, in writing or otherwise, to Facebook's collection, creation, storage, or use of her face template or any of her biometric information.

56. Plaintiff accordingly was never provided an opportunity to prohibit or prevent Facebook from collecting, storing, disclosing, or profiting from, or otherwise using her protected biometrics.

#### CLASS ACTION ALLEGATIONS

57. Plaintiff brings this lawsuit pursuant to Rule 23(b)(2) and (3) of the Federal Rules of Civil Procedure on behalf of the following proposed class (the "Class"):

***All Illinois residents who had their biometric identifiers, including scans of their face geometry collected, captured, received or otherwise obtained by Facebook through photographs uploaded to the Instagram app.***

58. Subject to additional information obtained through further investigation and discovery, the foregoing definition of the Class may be expanded or narrowed by amendment or amended complaint.

59. Specifically excluded from the Class are Defendant, its officers, directors, agents, trustees, parents, children, corporations, trusts, representatives, employees, principals, servants, partners, joint-venturers, or any entities controlled by Defendant, and its heirs, successors, assigns, or other persons or entities related to or affiliated with Defendant and/or its officers and/or directors, the judge assigned to this action, and any member of the judge's immediate family.



60. ***Numerosity.*** The members of the Class are so numerous that individual joinder is impracticable. Upon information and belief, plaintiff alleges that the Class contains many thousands of members. Although the precise number of Class members is unknown to plaintiff, the true number of Class members is known by Defendant, and thus, may be notified of the pendency of this action by first class mail, electronic mail and/or published notice.

61. ***Existence and predominance of common questions of law and fact.*** Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting only individual Class members. These common legal and factual questions include, but are not limited to, the following:

(a) whether Defendant collected, captured, received, or otherwise obtained biometric identifiers or biometric information from Plaintiff and the Class;

(b) whether Defendant informed Plaintiff and the Class before collecting, using, and storing their biometric identifiers or biometric information, as required by §15(b) the BIPA;

(c) whether Defendant informed Plaintiff and the Class of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored and used, as required by §15(b) the BIPA;

(d) whether Defendant obtained a written release, as defined by the BIPA, from Plaintiff and the Class to collect, store, and use their biometric identifiers or biometric information;

(e) whether Defendant used biometric identifiers to identify Plaintiff and the Class;

(f) whether Defendant provided a publicly available written policy

establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometrics information when the initial purpose for collecting such identifiers or information had been satisfied or within 3 years of the individual's last interaction with Facebook, as required by §15(a) of the BIPA;

(g) Whether Defendant sold, leased, traded, or otherwise profited from Plaintiff's or Class Members' biometric identifiers and biometric information in violation of §15(c) of the BIPA;

(h) Whether Defendant disclosed, redisclosed, or otherwise disseminated Plaintiff's and Class Members' biometric identifiers or biometric information in violation of §15(d) of the BIPA;

(i) Whether Defendant protected Plaintiff's and Class Members' biometric identifiers or biometric information from disclosure pursuant as required by §15(e) of the BIPA;

(j) whether Defendant's violations of the BIPA were committed intentionally, recklessly or negligently;

(k) whether Plaintiff and the Class are entitled to statutory damages under the BIPA and the correct measure of those damages; and

(l) whether Plaintiff and the Class are entitled to declaratory and injunctive relief.

62. **Typicality.** Plaintiff's claims are typical of the claims of the other members of the Class in that Defendant collected, stored and used his biometric information without informed consent in the exact same manner as every other Class member.

63. **Adequacy of representation.** Plaintiff will fairly and adequately protect the

interests of the Class. Plaintiff has retained counsel highly experienced in complex consumer class action litigation, and Plaintiff intends to vigorously prosecute this action. Further, Plaintiff has no interests that are antagonistic to those of the Class.

64. ***Superiority.*** A class action is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class members is relatively small compared to the burden and expense that would be entailed by individual litigation of their claims against Defendant. It would thus be virtually impossible for the Class, on an individual basis, to obtain effective redress for the wrongs committed against them. Furthermore, even if Class members could afford such individualized litigation, the court system could not. Individualized litigation would create the danger of inconsistent or contradictory judgments arising from the same set of facts. Individualized litigation would also increase the delay and expense to all parties and the court system from the issues raised by this action. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, economies of scale, and comprehensive supervision by a single court, and presents no unusual management difficulties under the circumstances here.

65. The Class may also be certified because:

(a) the prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudication with respect to individual Class members that would establish incompatible standards of conduct for the Defendant;

(b) the prosecution of separate actions by individual Class members would create a risk of adjudications with respect to them that would, as a practical matter, be dispositive of the interests of other Class members not parties to the adjudications, or

substantially impair or impede their ability to protect their interests; and/or

(c) Defendant has acted or refused to act on grounds generally applicable to the Class as a whole, thereby making appropriate final declaratory and/or injunctive relief with respect to the members of the Class as a whole.

### **COUNT I**

#### **Violations of the Illinois Biometric Information Privacy Act, 740 ILCS 14/15(a) (On Behalf of Plaintiff and the Class)**

66. Plaintiff realleges and incorporates by reference the allegations contained in the preceding paragraphs as though fully set forth herein.

67. Section 15(a) of the BIPA requires:

A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first.

740CS 14/15(a).

68. Facebook does not provide a publicly available retention schedule or guidelines for permanently destroying Instagram users' biometric identifiers and biometric information when the initial purpose for collecting such identifiers or information has been satisfied or within 3 years of the individual's last interaction with Facebook as required by the BIPA. Therefore, Facebook has violated §15(a) of the BIPA. Facebook's violations of §15(a) of the BIPA were intentional or reckless or, alternatively, negligent.

69. As a result of Facebook's violations of §15(a) of the BIPA, Plaintiff seeks the following relief individually and on behalf of the Class: (l) injunctive and equitable relief pursuant to 740 ILCS 14/20(4) requiring Facebook to comply with §15(a) of the BIPA's

requirement to establish and provide a publicly available retention schedule or guidelines for permanently destroying its users' biometric identifiers and biometric information; (2) statutory damages of \$5,000 for each intentional or reckless violation of §15(a) of the BIPA pursuant to 740 ILCS 14/20(2), or alternatively, statutory damages of \$1,000 per negligent violation of §15(a) of the BIPA pursuant to 740 ILCS 14/20(1); and (3) reasonable attorneys' fees and costs expenses pursuant to 740 ILCS 14/20(3).

## **COUNT II**

### **Violations of the Illinois Biometric Information Privacy Act, 740 ILCS 14/15(b) (On Behalf of Plaintiff and the Class)**

70. Plaintiff realleges and incorporates by reference the allegations contained in the preceding paragraphs as though fully set forth herein.

71. Section 15(b) of the BIPA provides that a private entity may not, among other things, collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers or biometric information, unless it first:

(1) informs the subject . . . in writing that a biometric identifier or biometric information is being collected or stored;

(2) informs the subject . . . in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and

(3) receives a written release executed by the subject of the biometric identifier or biometric information . . . .

740 ILCS 14/15(b).

72. Facebook is a private entity under the BIPA. *See* 740 ILCS 14/10.

73. Plaintiff and the Class members are individuals under the BIPA. *See id.*

74. Facebook collected Plaintiff's and the Class members' "biometric identifiers"

through its facial recognition software, as alleged above. *See id.*

75. Plaintiff's and the Class members' biometric identifiers collected by Facebook constitute "biometric information" as defined by the BIPA because Facebook used those biometric identifiers to identify Plaintiff and the Class members. *See id.*

76. Facebook systematically collected, used, and stored Plaintiff's and the Class members' biometric identifiers and biometric information without first obtaining the written release required by §15(b) of the BIPA.

77. As alleged above, Facebook did not inform Plaintiff or the Class members in writing that their biometric identifiers or biometric information were being collected, stored and used, as required by §15(b) of the BIPA.

78. As alleged above, Facebook did not inform Plaintiff or the Class members in writing of the specific purpose and length of term for which their biometric identifiers or biometric information was being collected, stored and used, as required by §15(b) of the BIPA.

79. By collecting, storing, and using Plaintiff's and the Class members' biometric identifiers and biometric information as described herein, Facebook violated Plaintiff's and the Class members' rights to privacy in their biometric identifiers or biometric information as set forth in the BIPA, 740 ILCS 14/1 et seq.

80. Facebook's violations of §15(b) of the BIPA were intentional or reckless because Facebook collected biometric data by default and without written notice as required by the BIPA and, therefore, Plaintiff and the Class members had no opportunity to provide Defendant with a written release, as mandated by the BIPA. Alternatively, Facebook's violations of §15(b) of the BIPA were negligent because Facebook failed to meet the applicable standard of care in ensuring that its members were informed and consented to the collection,

storage, and use of their biometric information and biometric identifiers.

81. As a result of Defendant's violations of §15(b) of the BIPA, Plaintiff seeks the following relief individually and on behalf of the Class: (1) injunctive and equitable relief pursuant to 740 ILCS 14/20(4) requiring Facebook to comply with the BIPA's requirements for the collection, storage, and use of biometric identifiers and biometric information as alleged herein; (2) statutory damages of \$5,000 for each intentional or reckless violation of the BIPA pursuant to 740 ILCS 14/20(2), or alternatively, statutory damages of \$1,000 per negligent violation of the BIPA pursuant to 740 ILCS 14/20(1); and (3) reasonable attorneys' fees and costs expenses pursuant to 740 ILCS 14/20(3).

### **COUNT III**

#### **Violations of the Illinois Biometric Information Privacy Act, 740 ILCS 14/15(c) (On Behalf of Plaintiff and the Class)**

82. Plaintiff realleges and incorporates by reference the allegations contained in the preceding paragraphs as though fully set forth herein.

83. Section 15(c) of the BIPA provides "[n]o private entity in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information."

84. As alleged above, Facebook violated BIPA by unlawfully profiting from individuals' biometric identifiers and biometric information, including the biometric identifiers and information of Plaintiff and Class Members.

85. Facebook's violations of BIPA were intentional and reckless or, pleaded in the alternative, negligent.

86. As a direct and proximate result of Facebook's violations of BIPA, Plaintiff and Class Members have suffered and will continue to suffer injury.

87. Plaintiff and Class Members seek as monetary relief the greater of \$5,000 or actual damages or, pleaded in the alternative, \$1,000 or actual damages.

88. Unless and until enjoined and restrained by order of this Court, Facebook's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class Members in that their biometric identifiers and information can be viewed and used by unauthorized persons. Plaintiff and Class Members have no adequate remedy at law for their injuries in that a judgment for monetary damages will not end the misuse of Plaintiff's and Class Member's biometric identifiers and information.

89. Plaintiff and Class Members also seek punitive damages, injunctive relief, and the reasonable attorney fees, costs, and expenses relating to this action.

#### **COUNT IV**

##### **Violations of the Illinois Biometric Information Privacy Act, 740 ILCS 14/15(d) (On Behalf of Plaintiff and the Class)**

90. Plaintiff realleges and incorporates by reference the allegations contained in the preceding paragraphs as though fully set forth herein.

91. Section 15(d) of the BIPA provides that "[n]o private entity in possession of a biometric identifier or biometric information may disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information [...]."

92. As alleged above, Facebook violated BIPA by disclosing and otherwise disseminating, upon information and belief, individuals' biometric identifiers and information, including the biometric identifiers and information of Plaintiff and Class Member, even though: (a) neither the subjects of the biometric identifiers and information nor their authorized representatives consented to the disclosure; (b) the disclosure did not complete a financial transaction requested or authorized by the subjects of the biometric identifiers and information



or their authorized representatives; (c) the disclosure was not required by State or federal law or municipal ordinance; and (d) the disclosure and redisclosure was not required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

93. Facebook's violations of BIPA were intentional and reckless or, pleaded in the alternative, negligent.

94. As a direct and proximate result of Facebook's violations of BIPA, Plaintiff and Class Members have suffered and will continue to suffer injury.

95. Plaintiff and Class Members seek as monetary relief the greater of \$5,000 or actual damages or, pleaded in the alternative, \$1,000 or actual damages.

96. Unless and until enjoined and restrained by order of this Court, Facebook's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class Members in that their biometric identifiers and information can be viewed and used by unauthorized persons. Plaintiff and Class Members have no adequate remedy at law for their injuries in that a judgment for monetary damages will not end the misuse of Plaintiff's and Class Member's biometric identifiers and information.

97. Plaintiff and Class Members also seek punitive damages, injunctive relief, and the reasonable attorney fees, costs, and expenses relating to this action.

#### **COUNT V**

#### **Violations of the Illinois Biometric Information Privacy Act, 740 ILCS 14/15(e) (On Behalf of Plaintiff and the Class)**

98. Plaintiff realleges and incorporates by reference the allegations contained in the preceding paragraphs as though fully set forth herein.

99. Section 15(e) of the BIPA provides that "[a] private entity in possession of a biometric identifier or biometric information shall:"

(1) store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity's industry; and

(2) store, transmit, and protect from disclosure all biometric identifiers and biometric information in a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information.

100. As alleged above, upon information and belief, Facebook violated BIPA because, while in possession of Plaintiff's and Class Members' biometric identifiers and information, it failed to protect from disclosure those biometric identifiers and information: (a) using the reasonable standard of care within Facebook industry; and (b) in a manner that is the same as or more protective than the manner in which Facebook protects and protected other confidential and sensitive information when it voluntarily disclosed the biometrics to third parties.

101. Facebook's violations of BIPA were intentional and reckless or, pleaded in the alternative, negligent.

102. As a direct and proximate result of Facebook's violations of BIPA, Plaintiff and Class Members have suffered and will continue to suffer injury.

103. Plaintiff and Class Members seek as monetary relief the greater of \$5,000 or actual damages or, pleaded in the alternative, \$1,000 or actual damages.

104. Unless and until enjoined and restrained by order of this Court, Facebook's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class Members in that their biometric identifiers and information can be viewed and used by unauthorized persons. Plaintiff and Class Members have no adequate remedy at law for their injuries in that a judgment for monetary damages will not end the misuse of Plaintiff's and Class Member's biometric identifiers and information.

105. Plaintiff and Class Members also seek punitive damages, injunctive relief, and the reasonable attorney fees, costs, and expenses relating to this action.

## **COUNT VI**

### **Unjust Enrichment (On Behalf of Plaintiff and the Class)**

106. Plaintiff realleges and incorporates by reference the allegations contained in the preceding paragraphs as though fully set forth herein.

107. Facebook obtained a monetary benefit from Plaintiff and Class Members to their detriment. Facebook did so by profiting off of the covert and unauthorized collection of the biometric identifiers and information of Plaintiff and Class Members, while exposing Plaintiff and Class Members to a heightened risk of privacy harms and depriving them of their control over their biometric data.

108. Plaintiff and Class Members did not authorize Facebook to collect, capture, obtain, disclose, redisclose, disseminate and otherwise profit off from their biometric identifiers and information.

109. Facebook appreciated, accepted, and retained the benefit bestowed upon it under inequitable and unjust circumstances arising from Facebook's conduct toward Plaintiff and Class Members as described herein.

110. Facebook sold, leased, traded, and/or otherwise profited from Plaintiff's and Class Members' biometric identifiers and information and did not provide full compensation for the benefit received from Plaintiff and Class Members.

111. Facebook acquired and caused to be acquired Plaintiff's and Class Members' biometric identifiers and information through inequitable means in that it collected, captured and

otherwise obtained biometric data from Plaintiff's and Class Members' online photos without permission and in violation of Illinois law.

112. Plaintiff and Class Members have no adequate remedy at law.

113. Under the circumstances, it would be unjust and unfair for Facebook to be permitted to retain any of the benefits obtained from Plaintiff and Class Members and their biometric identifiers and information.

114. Under the principles of equity and good conscience, Facebook should not be permitted to retain the biometric identifiers and information belonging to Plaintiff and Class Members because Facebook unlawfully obtained the biometric identifiers and information.

115. Facebook should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that it unjustly received as a result of its collection, capture, obtainment, disclosure, redisclosure, dissemination and profiting off of Plaintiff's and Class Members' biometric identifiers and information, including but not limited to the value of the intellectual property derived therefrom.

### **PRAYER FOR RELIEF**

WHEREFORE, Plaintiff prays for a judgment against Defendant as follows:

A. Certifying the Class as defined above, appointing Plaintiff as Class Representative, and appointing his undersigned counsel as Class counsel;

B. Declaring that Defendant's actions, as alleged above, violate §15(a) and (b) of the BIPA, 740 ILCS 14/1 *et seq.*;

C. Awarding statutory damages of \$5,000 for each intentional or reckless violation of the BIPA pursuant to 740 ILCS 14/20(2), or alternatively, statutory damages of \$1,000 per negligent violation of the BIPA pursuant to 740 ILCS 14/20(1);

D. Awarding injunctive and equitable relief pursuant to 740 ILCS 14/20(4) requiring Facebook to comply with the BIPA by providing a publicly available retention schedule or guidelines for permanently destroying its users' biometric identifiers and biometric information and forcing Defendant to stop collecting, storing, and using Plaintiff's and the Class members' biometric identifiers and biometric information without first obtaining their informed written consent;

E. An order requiring Facebook to disgorge into a common fund or constructive fund, for the benefit of Plaintiff and members of the proposed Class, proceeds that it unjustly received as a result of its collection, capture, obtainment, disclosure, dissemination, and profiting off of Plaintiff's and Class Members' biometric identifiers and information;

F. An award of pre-judgment and post-judgment interest for Plaintiff and members of the proposed Class, as permitted by law;

G. Awarding Plaintiff attorneys' fees and costs pursuant to 740 ILCS 14/20(3); and

H. Awarding any further relief as the Court may deem just and proper.

### **JURY DEMAND**

Plaintiff hereby demands a jury trial on all issues so triable.

Dated: August 14, 2020

/s/Gregory F. Coleman

Gregory F. Coleman (TN014092)

Lisa A. White\* (TN026658)

Jonathan B. Cohen (FL0027620)

GREG COLEMAN LAW PC

800 S. Gay Street, Suite 1100

Knoxville, TN 37929

Telephone: (865) 247-0080

Facsimile: (865) 522-0049  
greg@gregcolemanlaw.com  
lisa@gregcolemanlaw.com  
jonathan@gregcolemanlaw.com

*\*pro hac vice* to be filed